TRACK 1
INFORMATION SECURITY USER AWARENESS

State of Maryland

Security Awareness, Training, and Education (SATE) Program

INSTRUCTOR INFORMATION

- Name:
- Agency/Organization:
- Job Title:
- Contact Information:
  - Phone
  - E-mail

ADMINISTRATIVE ISSUES

- Track Duration
- Handouts
- Breaks
- Restrooms
- Cell Phones/Pagers/PDA’s
- End of Course Evaluation

MARYLAND'S INFORMATION SAT&E STRATEGY

Courses	Track 1 – User Awareness	Track 2 – Management Education	Track 3 – IT Staff Security Education
Audience	All State of Maryland Employees and Contractors	System/Application Owners, Security Officers	System/Application Administrators, Security Officers, Network Staff
Content	• Threats / Vulnerabilities • Acceptable Use / Rules of Behavior • Data Protection • Virus Prevention • Email Security • Telecommuting • Incident Reporting	• Risk Management • Disaster Recovery Planning • Incident Response Planning • Certification & Accreditation	• Threats, Vulnerabilities & Risks • Information Security Concepts & the State of Maryland Security Policy • Disaster & Incident Readiness • Incident Response

AGENDA

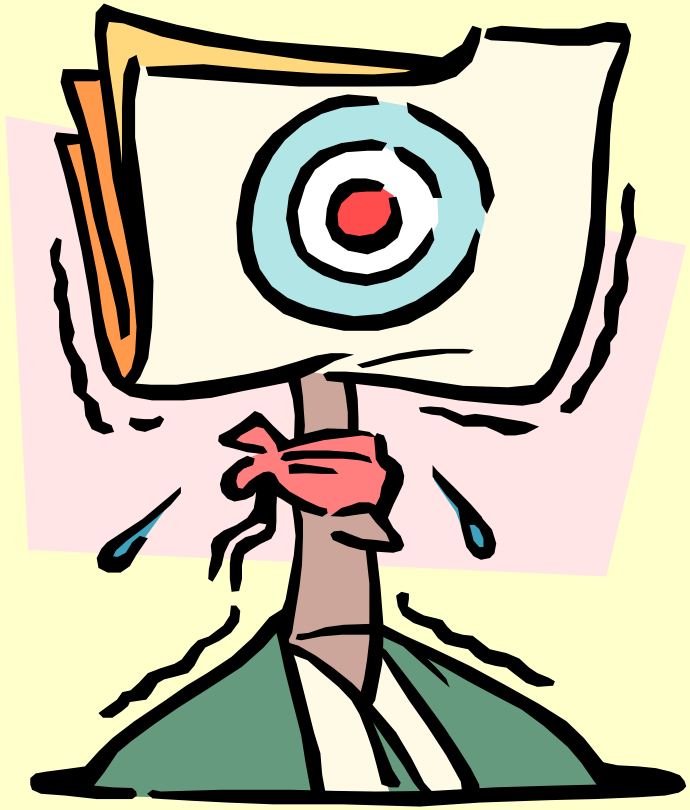
- Purpose
- Threats and Vulnerabilities
- Standards of Behavior
- Data Protection
- Virus Prevention
- E-Mail
- Telecommuting
- Incident Reporting

PURPOSE

- Information Security requires universal participation; you are part of the solution
- Increase and maintain the information security awareness of all State employees (including contractors) that access State Information Technology (IT) resources
- Comply with the State of Maryland Information Security Policy and Standards

COMMON MISCONCEPTIONS

- “We’ve never had an incident...”
- “My data isn’t that important.”
- “We have an open campus anyway, what’s the use?”



SECURITY REALITY

- 90% of respondents detected computer security breaches within the last twelve months.
- 80% acknowledged financial losses due to computer breaches.
- 74% cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

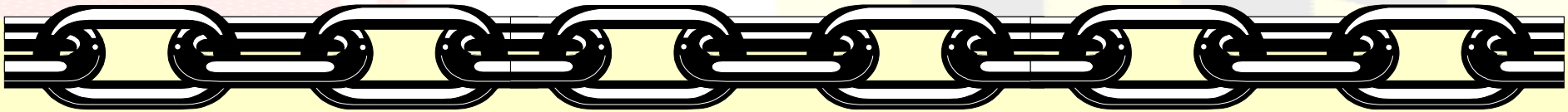
STATE OF MARYLAND SECURITY REQUIREMENT

Agencies shall develop and implement a security awareness, training, and education program for all Agency employees and contractors to ensure that all employees and contractors adhere to the State IT Security Policy and Standards.

STATE OF MARYLAND SECURITY PHILOSOPHY

Information and IT systems are assets of vital importance to the citizens, businesses and government of the State of Maryland. The security of information and information systems used by the State requires careful protection in order to maintain integrity of government operations and to safeguard private information.

THE SECURITY CHAIN



Links in the Chain

(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

Links in the Chain

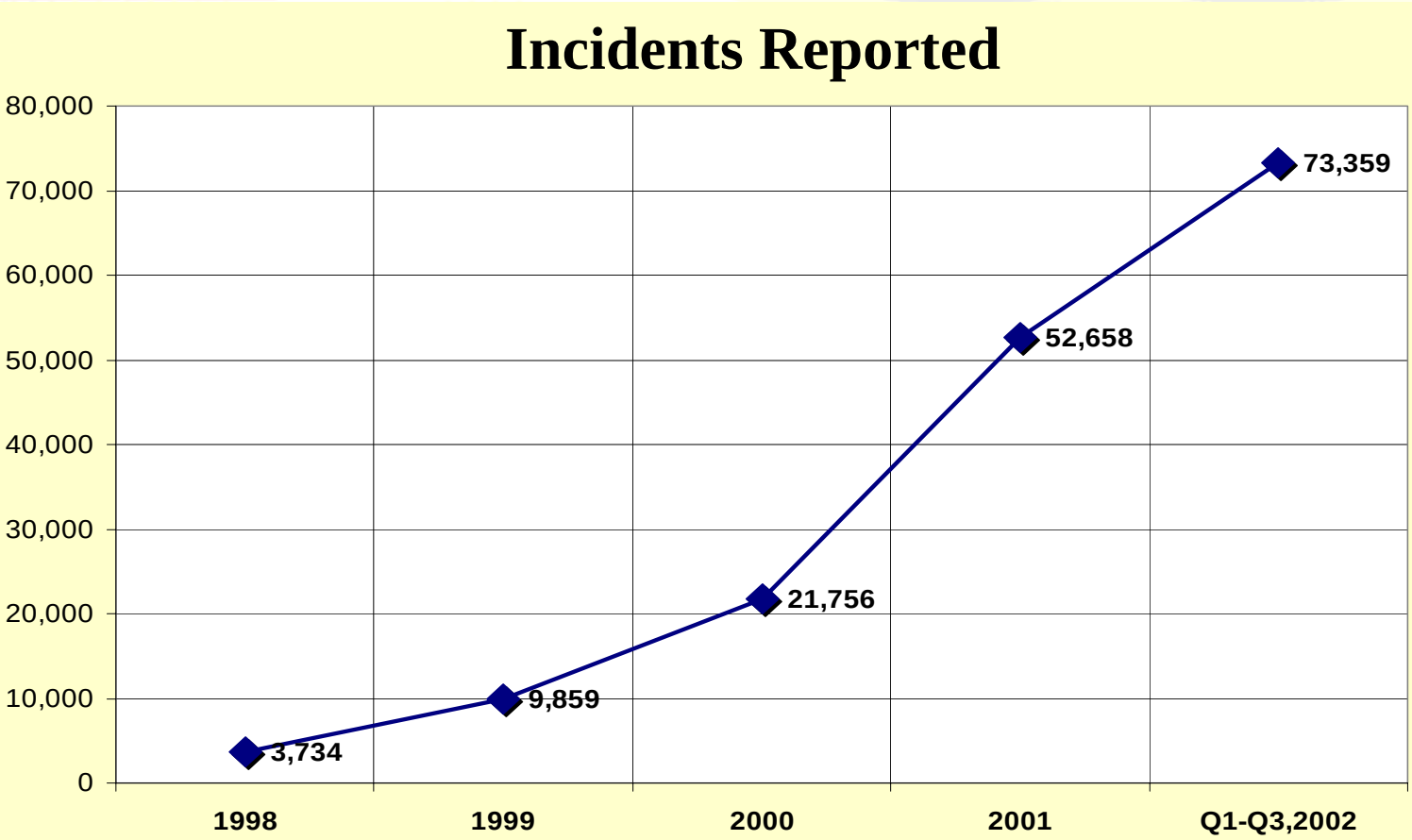
(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link…where is yours?

THREATS
AND
VULNERABILITIES

INCIDENTS ON THE RISE



Source: www.cert.org

THREAT

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability.

THREAT SOURCE

- A threat-source is defined as any circumstance or event with the potential to cause harm to an information technology system.
- Common threat-sources can be
  - Natural
  - Environmental
  - Human
  - Logical

NATURAL & ENVIRONMENTAL THREATS

- **Natural Threats**
  - Nature
    - Rain/Snow Storms
    - Earthquakes, Flood
    - Hurricane, Tornado
    - Lightning
  - Manmade/Accidental
    - Gas-line explosion
    - Water main rupture Electrical fire
- **Environmental Threats**
  - Loss of air conditioning
  - Loss of humidity controls

HUMAN THREATS

- Two classes of human threat sources:
  - Intentional - Intent and method targeted at the intentional exploitation of a vulnerability.
  - Unintentional - A situation and method that may accidentally trigger a vulnerability.

HUMAN INTENTIONAL
THREATS

- Insider Threats
  - Malicious Authorized User
  - Former Employees
- External Threats
  - Hackers/cracker/script kiddies
  - Foreign Intelligence Service
  - Terrorist

HUMAN INTENTIONAL
THREAT MOTIVATIONS

- Curiosity or challenge
- Intelligence collection
- Competitive edge or corporate espionage
- Revenge
- Vandalism
- Bragging
- Blackmail
- Theft
- Embezzlement

THREAT
SOCIAL ENGINEERING

- **DEFINITION** - The art and science of getting people to comply to your wishes.
- **GOAL** - To gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.
- **TECHNIQUES**
  - Phone
  - Dumpster Diving
  - Internet
  - Reverse Social Engineering

Hidden slide to continue notes.

THREAT
SOCIAL ENGINEERING

- **DEFINITION** - The art and science of getting people to comply to your wishes.
- **GOAL** - To gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.
- **TECHNIQUES**
  - Phone
  - Dumpster Diving
  - Internet
  - Reverse Social Engineering

CASE STUDY

ACCESSING THE CORPORATE NETWORK

- The strangers conducted days of research before attempting to enter the premises (learned key employee names by calling HR).
- They pretended to lose their building keys; an employee let them in.
- Claiming to have “lost" their identity badges for the “secured area”, another friendly employee let them in.
- They obtained financial data off of the CFO’s unlocked computer while he was out of town.
- The corporate trash yielded valuable documents, which they openly carried out of the building in a garbage pail provided by a janitor.
- The strangers phoned in pretending to be the CFO, desperate for his network password. Game Over! Hackers had access and soon gained super user access

MALICIOUS CODE
THREATS

- **Virus –** Three main traits: Replication, Concealment, and Bomb
- **Hoax –** Socially engineered virus
- **Trojan Horse –** Hides the true application within an expected or innocuous program
- **Worm –** Typically resides in memory and uses network services to replicate

Hidden slide to continue notes.

MALICIOUS CODE
THREATS

- **Virus –** Three main traits: Replication, Concealment, and Bomb
- **Hoax –** Socially engineered virus
- **Trojan Horse –** Hides the true application within an expected or innocuous program
- **Worm –** Typically resides in memory and uses network services to replicate

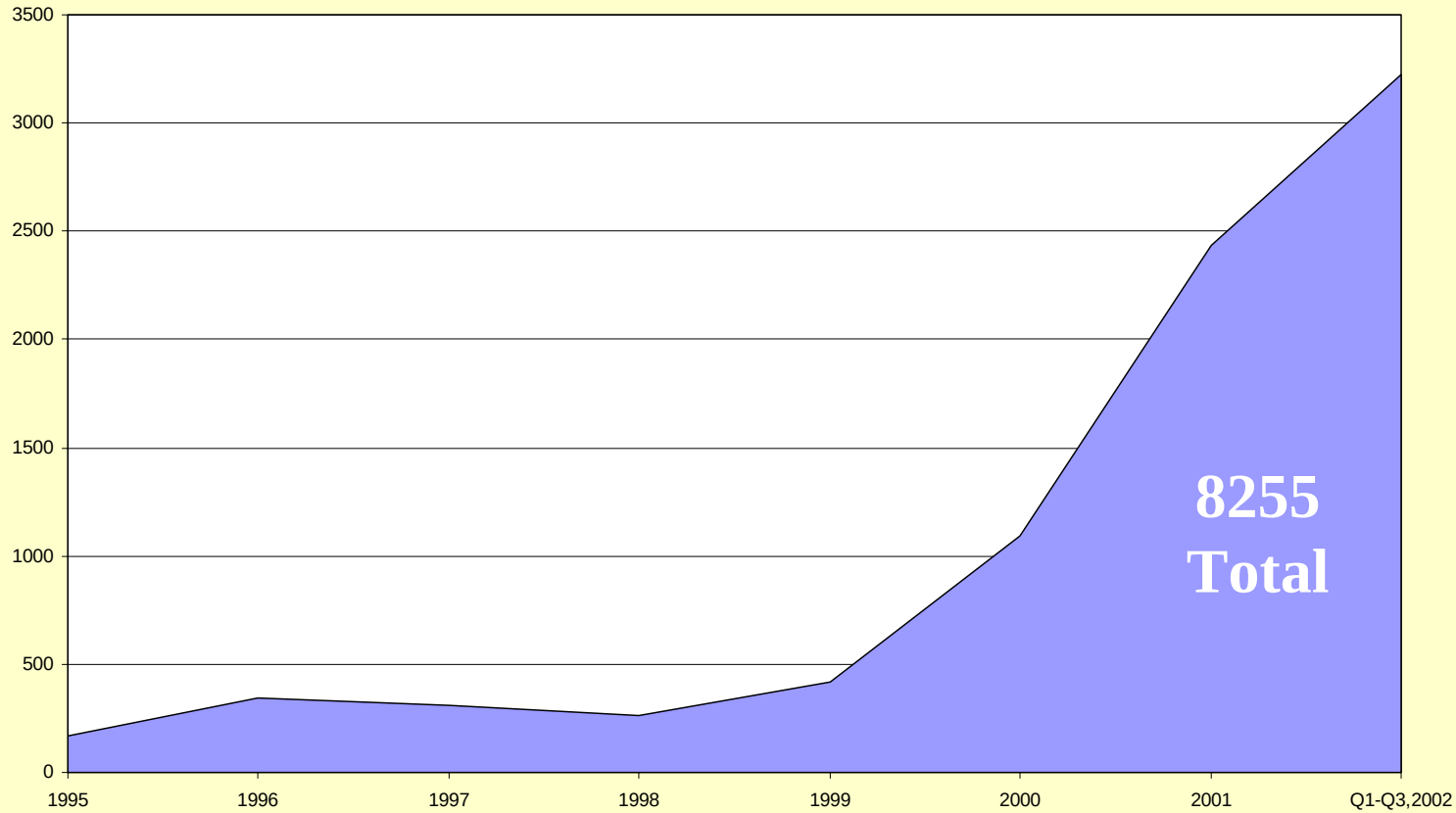
HUMAN UNINTENTIONAL THREAT

- Accidents
- Operational/procedural errors or omissions
- Negligence
- Non-availability of key personnel
- Improper software configuration

VULNERABILITY

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

VULNERABILITIES REPORTED



Source: cert.org

ACCEPTABLE USE STANDARD AND RULES OF BEHAVIOR

LEGAL NOTICE
(AKA: WARNING BANNER)

"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All transactional records, reports, e-mail, software, and other date generated by or residing upon this system are the property of the State of Maryland and may be used by the State of Maryland for any purpose."

RESPONSIBLIES
EMPLOYEES & CONTRACTORS

- Be aware of your responsibilities for protecting the IT assets of our Agency and the State.
- Exercise due diligence in carrying out the State's and your organization's policy, standards, and procedures.
- Understand that you are accountable for your actions relating to the use of State and Agency IT systems.
- Use IT resources only for intended purposes as defined by policies, laws and regulations of the State and your organization.

ACCEPTABLE USE STANDARD

- The use of State computing equipment, networks and communication facilities are provided to State employees and contract employees as electronic tools to meet their job functions.
- Email
  - Email is property of the State
  - State has authority to review and disclose contents to supervisory staff
  - Do not send PPI data unencrypted

ACCEPTABLE USE STANDARD

- Internet
  - Use is monitored by State
  - Improper use may be subject to legal action
- Downloading
  - Unauthorized software downloading is prohibited
- Non-Business Activities
  - Incidental non-business use may be permitted by Agency
  - May not conflict with aims and purposes of State

Hidden slide to continue notes.

ACCEPTABLE USE STANDARD

- Internet
  - Use is monitored by State
  - Improper use may be subject to legal action
- Downloading
  - Unauthorized software downloading is prohibited
- Non-Business Activities
  - Incidental non-business use may be permitted by Agency
  - May not conflict with aims and purposes of State

SOFTWARE
UNAUTHORIZED & PIRACY

- All software (i.e., operating system, applications, tools, etc.) must be owned by the State as a ***licensed copy*.**
- Other software is not authorized on State computers without express, written authorization.
- Any software found becomes the property of the State.
- Commercially procured software may not be duplicated/copied for any reason.

RULES OF BEHAVIOR
EMPLOYEES AND CONTRACTORS

- Comply with your access privileges
- Do not discuss sensitive data with anyone but authorized persons
- Secure the physical environment of your workstation
- Ensure printed and electronic media containing PPI data is properly handled during utilization and disposal
- Utilize available tools that enhance security

RULES OF BEHAVIOR
EMPLOYEES AND CONTRACTORS

- Never connect your workstation to another computer or electronic device
- Never download sensitive files to a medium that cannot be properly secured
- Never use a disk of unknown origin
- Participate in all required security training
- Report discovered or suspected vulnerabilities or breach-of-security incidents to your manager or the Help Desk

PASSWORD MANAGEMENT
"MUSTs"

- All accounts will have a password
- Selected by user or randomly generated
- Changed by user upon first login
- Minimum of eight characters, alpha-numeric
- Changed every 45 days
- Lock-out account after four failed login attempts

PASSWORD MANAGEMENT

"MUST NOTs"

- Be the same as your User Name (UserID)
- Be displayed as plaintext
- Consist of all numbers, all special or all alpha characters, or contain any null characters (blank spaces)
- Be reused within six months after changing to a new password (password history)
- Contain more than two consecutive (repeating) characters
- Be similar to previous passwords

PASSWORD MANAGEMENT
SECURITY MEASURES

- Don’t write down your password(s).
- Don’t share your password – you are responsible for any activities associated with your unique identifier and password.
- Don’t use personal data such as names, dates, places for your password that may be traced to you.

DATA PROTECTION

STATE OF MARYLAND
DATA SENSITIVITY

- **Public (PUB) -** Data that may be fully disclosed to the general public.
- **Proprietary and/or Protected Information (PPI) -** Data that is considered as sensitive to the owning Agency or State. Three categories of PPI:
  - High
  - Medium
  - Basic

STATE OF MARYLAND
PPI CATEGORIES

- **HIGH:** *Extremely sensitive* data within the agency and is intended for use only by named staff within the Agency.
- **MEDIUM:** *Sensitive* data within an agency and is intended for use only by specified groups of staff within the Agency.
- **LOW:** *Generally available* data to staff and non-staff employed by the Agency.

PROTECTING PPI DATA

- **Marking:** Mark with the highest classification contained on media
- **Transmitting :** PPI-HIGH must be encrypted
- **Storage:** Must be secured consistent with data sensitivity
- **Reuse:** Overwrite before reuse
- **Destruction:** PPI media destroyed in accordance with NIST Standards

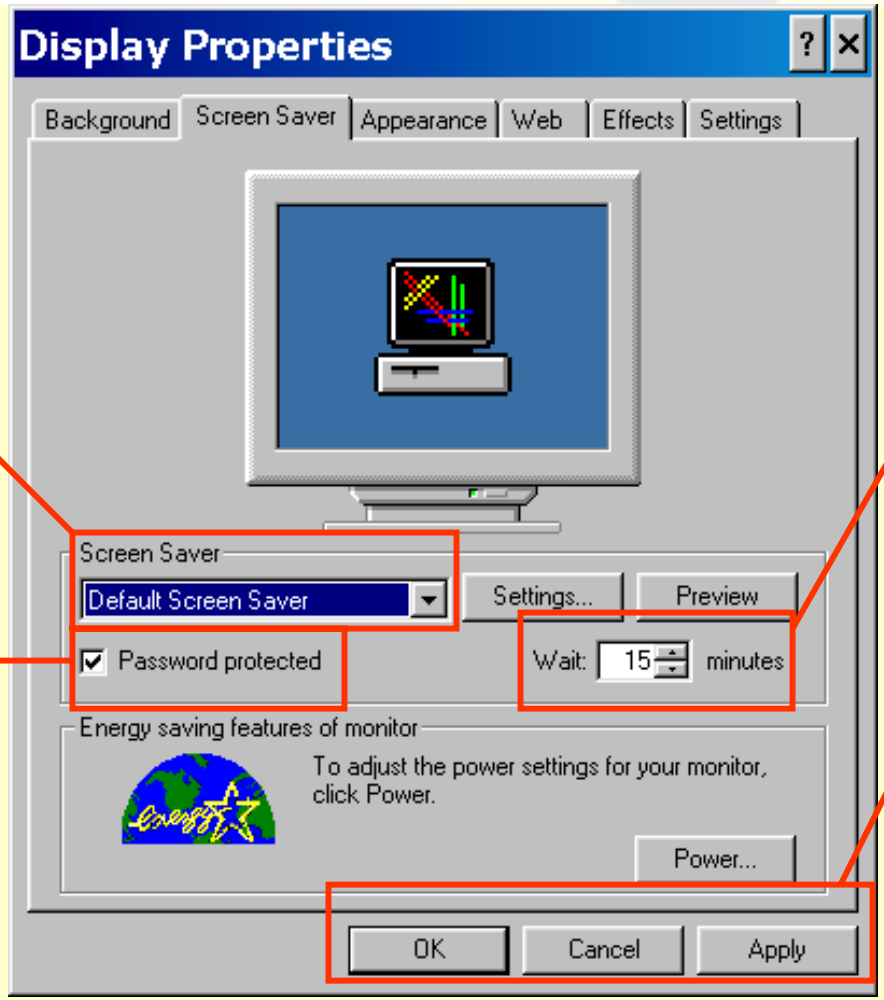
WORKSTATION SECURITY

- Log out when no longer needed for use (end of day)
- Lock your system whenever leaving the area
- Password protected screensaver

PASSWORD PROTECTED SCREENSAVER

1 - Scroll down and select one of the available screen savers.

2 – Check the password protected box.



3 – Set the time before screen saver automatically activates.

4 – Click the Apply button, then click the OK button

VIRUS PREVENTION

MALICIOUS LOGIC
DEFINITION

Hardware, software, or firmware capable of performing an unauthorized function on an IS.

NSTISSI 4009

A virus is only *one* type of malicious logic

MALICIOUS LOGIC
INDICATORS

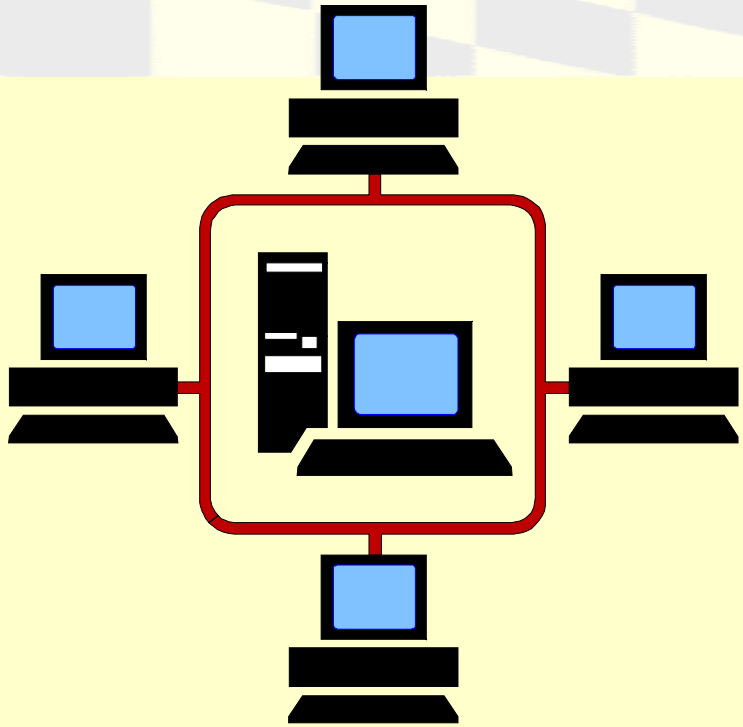
- Programs or files mysteriously disappearing
- Less memory available than usual
- Obsolete user accounts in use
- Executable files changing size for no apparent reason
- Unusual network activity
- Any unexplained messages or graphics on the screen
- An increase in the time required loading or executing a program
- An increase in the time required for disk accesses or processing
- Unusual error messages

MALICIOUS LOGIC
SOURCES

- "Intentional, human" threat
- Need not be programmers
  - Virus toolkits
  - Macro languages

- Vandals continue to produce malicious logic, then deliberately "set it loose"

MALICIOUS LOGIC
SOURCES OF INFECTION



- Propagate by machine or by human
  - Can spread quickly via networks
  - Usually, humans unintentionally spread malicious logic from one machine to another

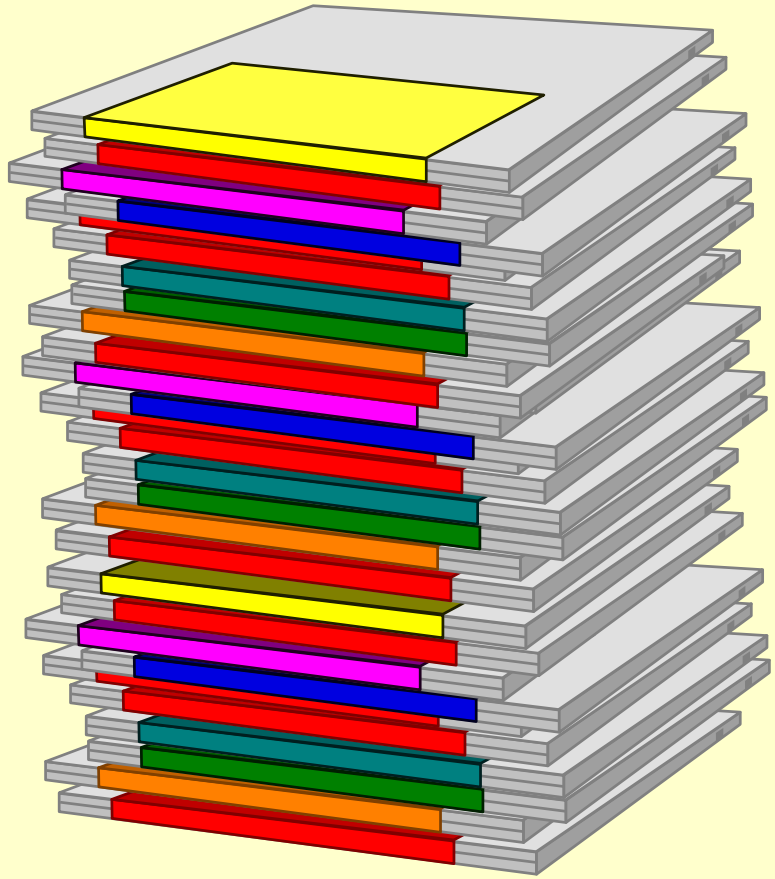
MALICIOUS CODE
PREVENTION: SOFTWARE

- Public Domain Software
- Low Risk - Authorized software
- High Risk - Unauthorized software
- Scanning Policy
- Unauthorized Software
- Imbedded Software

MALICIOUS CODE
PREVENTION: BACKUPS

"Three Rules of Computing"

- ***Make Backups***
- ***Make Backups***
- ***MAKE BACKUPS !!***



ANTI-VIRUS SOFTWARE

- Use Anti-Viral Software
  - Central implementation
  - Update
- Types
  - Signature scanner
  - Heuristic

ELECTRONIC MAIL
(E-Mail)

STATE OF MARYLAND
ACCEPTABLE USE STANDARD

- Email is a tool to meet a job function.
- Subject to State laws, regulations policies and other requirements.
- Email is the property of the State.
- Supervisors have the authority to determine when personal use is more than incidental, occasional or otherwise inappropriate.
- Email that is not secure or encrypted should not be used to send information that is PPI.

STATE OF MARYLAND
ACCEPTABLE USE STANDARD

- Incidental and occasional personal use of email is permitted at the discretion of the Agency when it:
  - Does not otherwise violate law, regulation or policy
  - Does not interfere with normal business activities
  - Does not involve solicitation
  - Is not associated with any for-profit outside business activity
  - Will not potentially embarrass the State or Agency

E-MAIL THREATS

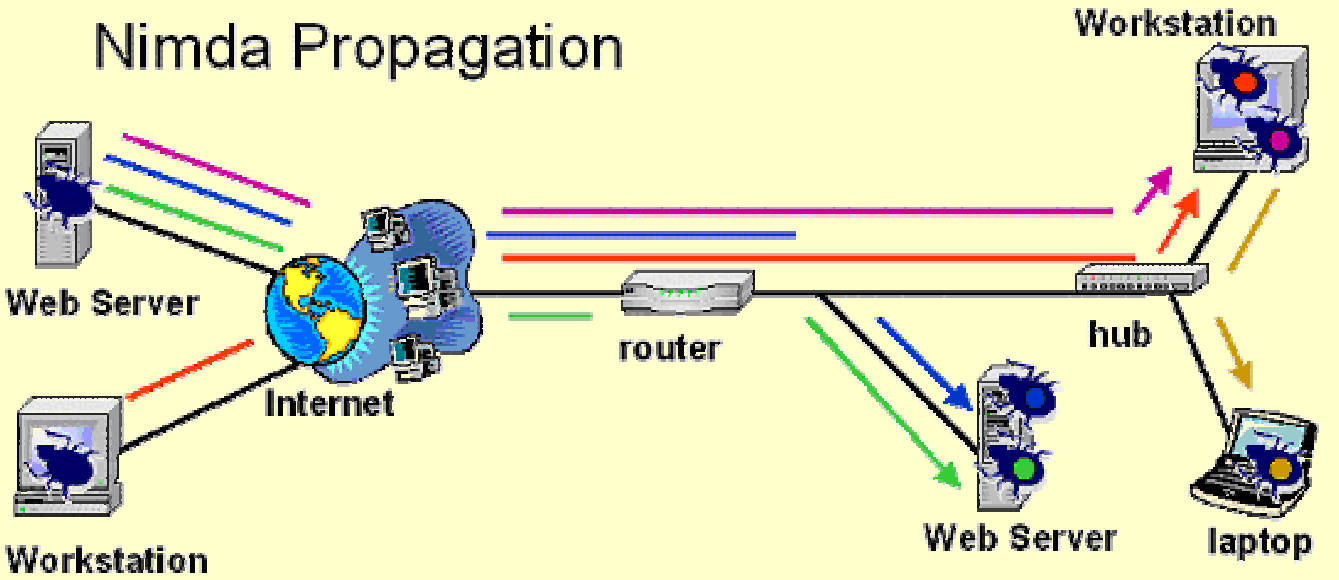
- Email spoofing
  - Email from alleged system administrator
  - Email form supervisor requesting sensitive data
- Email borne viruses
  - W32/Sircam
  - W32/Goner
- Hidden file extensions
  - Some email-borne viruses are known to exploit hidden file extensions

Hidden slide to continue notes.

E-MAIL THREATS

- Email spoofing
  - Email from alleged system administrator
  - Email form supervisor requesting sensitive data
- Email borne viruses
  - W32/Sircam
  - W32/Goner
- Hidden file extensions
  - Some email-borne viruses are known to exploit hidden file extensions

NIMDA
JUST ONE EXAMPLE



EMAIL DOs

- Use a different password for your e-mail than your network password (when possible).
- Save known email attachments to hard disk and scan them with an anti-virus program before opening.
- Create e-mail filtering rules to handle unsolicited mail (junk mail and spam).
- Discourage others from sending any attachments that are not business-related.

EMAIL DON'Ts

- **Don't** allow others to use your email account to send mail
- **Don't** open email from unknown sources
- **Don't** send sensitive information unencrypted (organizational information designated PPI)
- **Never** send any username or password
- **Never** run a program of unknown origin
- **Don't** use the State's email system for non-business related email

UNATHORIZED USE OF EMAIL

- Disparaging statements and remarks
- Threats – of any kind
- Messages sent to non-business related bulletin boards, news groups, or chat groups
- Chain letters
- Language that violates the State's policies on harassment

AVOIDING UNSOLICITED EMAIL (SPAM)

- Only give your email address to trusted parties.
- Notify you email administrator if you do receive Spam.
- If you receive Spam, delete it and go on with your business.
- Create filters for offensive Spam.

MINIMIZING SPAM

- **Never** give out your State email address unless you are required or desire to do for business purposes.
- **Never** subscribe to a mailing list that is not business related.
- **Never** use your State email address to purchase or obtain information on the Internet that is not business related.
- **Never** reply, reply to all, forward, unsubscribe, or do anything with it. Simply delete it.

TELECOMMUTING

TELECOMMUTING

- State law requires each agency to meet the participation goal of allowing 10% of all “eligible employees” to Telework.
- Allows employee (with supervisor approval) to work at home, a satellite office or at a Telework Center on selected work days.

TELECOMMUTING SECURITY

- Telework is responsible for the security of all items furnished by the State.
- Protection of sensitive information must be maintained per Agency-specified guidelines.
- The off-site workstation must comply with all security precautions identified throughout this lesson, as minimum requirements.
- Dial-in users shall not store either PUB or PPI, unless the data can be protected from unauthorized access, disclosure, modification, or destruction.

INCIDENT REPORTING

EXAMPLES

- A userid/password being used by a person other than the individual to whom that ID was assigned.
- Mishandling of sensitive data, reports, or storage media that may result in unauthorized personnel having access to same.
- An unexplained loss of disk space.
- The possibility of a computer virus.
- Theft of any network resources in the work area.
- Use of illegitimate or unauthorized copies of software.

USER INCIDENT REPORTING

- Whom to report to
- How to report
- What to report
  - The nature of the incident
  - When, where, how
  - Who discovered
  - Impact

STATE OF MARYLAND'S COMPUTER INCIDENT RESPONSE CAPABILITY (M-CIRC)

- Focal point for receiving computer security incident reports from State of Maryland Agencies
- Interface with reporting entities to collect relevant incident information
  - Record and track the incident reports
  - Provide initial incident assessment, triage, and handling recommendations.
- Provide incident report data to authorized State of Maryland personnel

M-CIRC CONT.

- Facilitates the creation and distribution of sanitized and generalized informational notices to State Agencies.
- Escalates incident reports to authorized State of Maryland personnel.
- Facilitates communication with external entities as directed.

SUMMARY

- Purpose
- Threats and Vulnerabilities
- Standards of Behavior
- Data Protection
- Virus Prevention
- E-Mail
- Telecommuting
- Incident Reporting


Questions

REFERENCES

State of Maryland:

- State of Maryland Information Technology Security Policy and Standards, Version 11, *Draft*, 10/08/02
- State of Maryland Executive Order (EO) 01.01.1983.18, Privacy and State Data System Security
- State of Maryland Information Technology Reform Plan
- State of Maryland Teleworker's Manual, March 2001

REFERENCES
Cont.

Federal:

- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security Glossary
- President's Executive Order (EO) 13231, Critical Infrastructure Protection in the Information Age
- Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection
- PDD 67, Enduring Constitutional Government and Continuity of Government Operations

REFERENCES
Cont.

- Computer Security Act of 1987 (Public Law (P.L. 100-235)
- Privacy Act of 1974 (P.L. 93-579)
- Computer Fraud and Abuse Act of 1986 (P.L. 99-474)
- Information Technology Reform Act of 1996 (P.L. 104-231)
- Freedom of Information Act (FOIA) of 1974 (P.L. 104-231)
- Government Information Security Reform Act (GISRA) of 2000 (P.L. 106-398)
- Federal Information Processing Standard (FIPS) 73, Guidelines for Security of Computer Applications

REFERENCES
Cont.

- FIPS 87, Guidelines for ADP Contingency Planning
- FIPS 112, Password Usage
- National Institute of Standards and Technology (NIST) Special Publication (SP) 500-171, Computer Users' Guide to the Protection of Information Resources
- NIST SP 800-9, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook

REFERENCES
Cont.

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-45, *Draft* Guidelines on Electronic Mail (E-Mail) Security
- NIST SP 800-50, *Draft* Building an Information Technology Security Awareness Program